(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11167487 A**

(43) Date of publication of application: **22.06.99**

(51) Int. Cl **G06F 9/06**
G06F 13/00
G06F 13/00
G06F 15/00

(21) Application number: **09331409**

(22) Date of filing: **02.12.97**

(71) Applicant: **FUJITSU LTD**

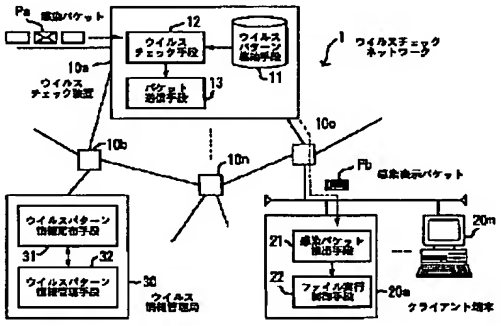
(72) Inventor: **NOJIRI NATSUKI**

(54) VIRUS CHECK NETWORK, VIRUS CHECK DEVICE, CLIENT TERMINAL AND VIRUS INFORMATION MANAGING STATION

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a virus check network with improved efficiency to prevent viruses on a network side.

SOLUTION: A virus pattern housing means 11 houses virus patterns. A virus check means 2 executes virus check whether a packet is an infected packet Pa or not based on the virus patterns on the network side. At the time of detecting an infected packet Pa, a packet transmitting means 13 stands a bit showing infection within the packet and transmits it as an infection displaying packet Pb. An infected packet detecting means 21 detects the infected packet. A file execution control means 22 makes a file execution-disable corresponding to the infected packet. A virus pattern information delivering means 31 delivers virus pattern information to virus check devices 10a to 10n by multicasting. A virus pattern information managing means 32 uniformly manages virus pattern information.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－167487

(43)公開日　平成11年(1999)６月22日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	9/06	５５０	Ｇ０６Ｆ	9/06	５５０Ｚ
	13/00	３５１		13/00	３５１Ｚ
		３５５			３５５
	15/00	３３０		15/00	３３０Ａ

審査請求　未請求　請求項の数12　ＯＬ　（全 14 頁）

(21)出願番号　特願平9－331409

(22)出願日　平成９年(1997)12月２日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　野尻　夏樹
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

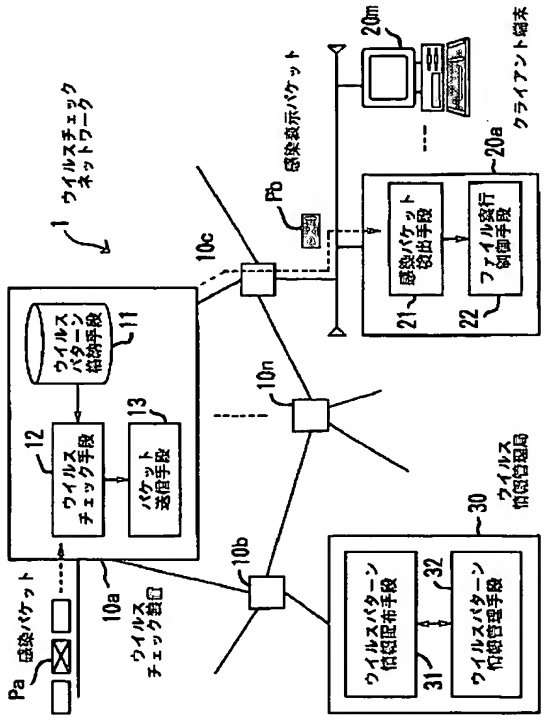
(74)代理人　弁理士　服部　毅巖

(54)【発明の名称】　ウィルスチェックネットワーク、ウィルスチェック装置、クライアント端末及びウィルス情報管理局

(57)【要約】

【課題】　ネットワーク側でウィルスを未然に防ぎ、ウィルス対策効率の向上を図ったウィルスチェックネットワークを提供することを目的とする。

【解決手段】　ウィルスパターン格納手段１１は、ウィルスパターンを格納する。ウィルスチェック手段１２は、パケットをウィルスパターンにもとづいて、感染パケットＰａか否かのウィルスチェックをネットワーク側で行う。パケット送信手段１３は、感染パケットＰａ検知時は、パケット内の感染を示すビットを立てて感染表示パケットＰｂとして送信する。感染パケット検出手段２１は、感染パケットＰａを検出する。ファイル実行制御手段２２は、感染パケットに対応するファイルを実行不可にする。ウィルスパターン情報配布手段３１は、ウィルスパターン情報をマルチキャストでウィルスチェック装置１０ａ～１０ｎに配布する。ウィルスパターン情報管理手段３２はウィルスパターン情報を一元管理する。



1

【特許請求の範囲】

【請求項１】　ウィルスチェックを行って、ウィルス侵入を防止するウィルスチェックネットワークにおいて、

ウィルスパターンを格納するウィルスパターン格納手段と、受信したパケットを前記ウィルスパターンにもとづいて、ウィルスに感染している感染パケットか否かの前記ウィルスチェックをネットワーク側で行うウィルスチェック手段と、前記感染パケットを検知した場合は、感染を示すパケット内のビットを立てて感染表示パケットとして送信するパケット送信手段と、から構成される複数のウィルスチェック装置と、

前記ビットにもとづいて、前記感染パケットを検出する感染パケット検出手段と、前記感染パケットに対応するファイルを実行不可にするファイル実行制御手段と、から構成されるクライアント端末と、

ウィルスパターン情報をマルチキャストで前記ウィルスチェック装置に配布するウィルスパターン情報配布手段と、前記ウィルスパターン情報を一元管理するウィルスパターン情報管理手段と、から構成されるウィルス情報管理局と、

を有することを特徴とするウィルスチェックネットワーク。

【請求項２】　前記ウィルスチェック手段は、前記パケットのヘッダを見て前記ウィルスチェックすべき前記パケットを選定することを特徴とする請求項１記載のウィルスチェックネットワーク。

【請求項３】　前記ウィルスチェック装置は、ルータに配置されることを特徴とする請求項１記載のウィルスチェックネットワーク。

【請求項４】　前記ウィルスチェック装置は、前記ウィルスパターン情報を前記マルチキャストで互いに通知することを特徴とする請求項１記載のウィルスチェックネットワーク。

【請求項５】　前記ウィルスチェック装置は、前記ウィルスの脅威レベルに応じて警戒モードを設定し、ホストとの通信を一定時間遮断させる警戒モード設定手段をさらに含むことを特徴とする請求項１記載のウィルスチェックネットワーク。

【請求項６】　前記ウィルスチェック装置は、前記ウィルスチェックを行う部位を複数設け、前記ウィルスチェック装置毎に担当するウィルスチェック領域を分担することを特徴とする請求項１記載のウィルスチェックネットワーク。

【請求項７】　前記ウィルスチェック装置は、ネットワーク上新規に置かれた場合は、他の前記ウィルスチェック装置から前記ウィルスチェックの担当領域情報を収集することを特徴とする請求項６記載のウィルスチェックネットワーク。

【請求項８】　前記パケット送信手段は、前記感染表示パケットの送信と共に、前記感染パケットの送信元に警

2

告パケットを送信し、かつ他の前記ウィルスチェック装置に警戒すべき前記感染パケットの情報が記された警戒情報パケットをマルチキャストで配布することを特徴とする請求項１記載のウィルスチェックネットワーク。

【請求項９】　前記ウィルスチェック手段は、前記警戒情報パケットに記された前記感染パケットの前記ウィルスパターンの優先順位を上げて、前記ウィルスチェックを行うことを特徴とする請求項８記載のウィルスチェックネットワーク。

【請求項１０】　ウィルスチェックを行って、ウィルス侵入を防止するウィルスチェック装置において、

ウィルスパターンを格納するウィルスパターン格納手段と、

受信したパケットを前記ウィルスパターンにもとづいて、ウィルスに感染している感染パケットか否かの前記ウィルスチェックをネットワーク側で行うウィルスチェック手段と、

前記感染パケットの場合は、感染を示すパケット内のビットを立てて感染表示パケットとして送信するパケット送信手段と、

を有することを特徴するウィルスチェック装置。

【請求項１１】　ウィルスチェックを受けたパケットを受信するクライアント端末において、

ウィルスに感染されていることを示すビットが立っているパケットを感染パケットとして検出する感染パケット検出手段と、

前記感染パケットを検出した場合は、対応するファイルを実行不可にするファイル実行制御手段と、

を有することを特徴するクライアント端末。

【請求項１２】　ネットワーク内のウィルス情報を管理するウィルス情報管理局において、

ウィルスパターン情報を前記ネットワーク内に配置されたウィルスチェクを行うウィルスチェック装置にマルチキャストで配布するウィルスパターン情報配布手段と、

前記ウィルスパターン情報を一元管理するウィルスパターン情報管理手段と、

を有することを特徴するウィルス情報管理局。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はウィルスチェックネットワーク、ウィルスチェック装置、クライアント端末及びウィルス情報管理局に関し、特にウィルスチェックを行って、ウィルス侵入を防止するウィルスチェックネットワーク、ウィルスチェックを行って、ウィルス侵入を防止するウィルスチェック装置、ウィルスチェックを受けたパケットを受信するクライアント端末及びネットワーク内のウィルス情報を管理するウィルス情報管理局に関する。

【０００２】

【従来の技術】近年、マルチメディア通信などの情報通

信ネットワーク技術が急速に進歩している。また、インターネット等の流行により、企業のみならず一般家庭に対しても、ネットワークが提供するサービスが幅広く利用されている。

【０００３】この反面、コンピュータウィルスの増加と感染のスピードは、ネットワークの普及と共に加速しており、多くの企業ユーザがウィルスの被害に遭っている現状が報告されている。

【０００４】従来、ネットワークをウィルスの感染から守るには、クライアントやプロキシサーバ等にワクチン・ソフトを導入していた。このワクチン・ソフトを用いることにより、ウィルスに感染しているファイルからウィルスを取り去って、ファイルを修復することができる。

【０００５】

【発明が解決しようとする課題】しかし、上記のような従来のウィルス対策は、クライアント側で行っているため、感染防止にはクライアントすべてに対して、個々にワクチン・ソフトを導入しなければならない。

【０００６】このため、新種ウィルスに対しては、バージョンアップしたワクチン・ソフトを最初から逐一導入しなければならず、時間が非常にかかり効率が悪いといった問題があった。

【０００７】また、従来のクライアント側でのウィルス対策では、新種ウィルス発見時のパターンファイルの更新などをはじめとする運用管理等は、各自ユーザに任されるため、ウィルス監視を徹底させることが難しいといった問題があった。

【０００８】本発明はこのような点に鑑みてなされたものであり、ネットワーク側でウィルスを未然に防ぎ、ウィルス対策効率の向上を図ったウィルスチェックネットワークを提供することを目的とする。

【０００９】また、本発明の他の目的は、ネットワーク側でウィルスを未然に防ぎ、ウィルス対策効率の向上を図ったウィルスチェック装置を提供することである。さらに、本発明の他の目的は、ウィルスに感染しているファイルを削除して、ウィルス対策効率の向上を図ったクライアント端末を提供することである。

【００１０】また、本発明の他の目的は、ネットワーク内のウィルス情報を管理して、ウィルス対策効率の向上を図ったウィルス情報管理局を提供することである。

【００１１】

【課題を解決するための手段】本発明では上記課題を解決するために、図１に示すような、ウィルスチェックを行って、ウィルス侵入を防止するウィルスチェックネットワーク１において、ウィルスパターンを格納するウィルスパターン格納手段１１と、受信したパケットをウィルスパターンにもとづいて、ウィルスに感染している感染パケットＰａか否かのウィルスチェックをネットワーク側で行うウィルスチェック手段１２と、感染パケット

Ｐａを検知した場合は、感染を示すパケット内のビットを立てて感染表示パケットＰｂとして送信するパケット送信手段１３と、から構成される複数のウィルスチェック装置１０ａ～１０ｎと、ビットにもとづいて、感染パケットＰａを検出する感染パケット検出手段２１と、感染パケットＰａに対応するファイルを実行不可にするファイル実行制御手段２２と、から構成されるクライアント端末２０ａ～２０ｍと、ウィルスパターン情報をマルチキャストでウィルスチェック装置１０ａ～１０ｎに配布するウィルスパターン情報配布手段３１と、ウィルスパターン情報を一元管理するウィルスパターン情報管理手段３２と、から構成されるウィルス情報管理局３０と、を有することを特徴とするウィルスチェックネットワーク１が提供される。

【００１２】ここで、ウィルスパターン格納手段１１は、ウィルスパターンを格納する。ウィルスチェック手段１２は、受信したパケットをウィルスパターンにもとづいて、ウィルスに感染している感染パケットＰａか否かのウィルスチェックをネットワーク側で行う。パケット送信手段１３は、感染パケットＰａを検知した場合は、感染を示すパケット内のビットを立てて感染表示パケットＰｂとして送信する。感染パケット検出手段２１は、ビットにもとづいて、感染パケットＰａを検出する。ファイル実行制御手段２２は、感染パケットに対応するファイルを実行不可にする。ウィルスパターン情報配布手段３１は、ウィルスパターン情報をマルチキャストでウィルスチェック装置１０ａ～１０ｎに配布する。ウィルスパターン情報管理手段３２は、ウィルスパターン情報を一元管理する。

【００１３】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照して説明する。図１は本発明のウィルスチェックネットワークの原理図である。

【００１４】ウィルスチェックネットワーク１は、ウィルスチェック装置１０ａ～１０ｎと、クライアント端末２０ａ～２０ｍと、ウィルス情報管理局３０と、から構成され、ウィルスチェックを行って、ウィルス侵入を防止する。

【００１５】ウィルスパターン格納手段１１は、ウィルスパターンを格納する。ウィルスチェック手段１２は、受信したパケットと、格納してあるウィルスパターンと、を比較し、パケットがウィルスに感染している感染パケットＰａか否かのウィルスチェックをネットワーク側で行う。

【００１６】パケット送信手段１３は、感染パケットＰａを検知した場合は、感染パケットＰａ内のあらかじめ設定した感染を示すビットを立てて、感染表示パケットＰｂとして送信する。

【００１７】感染パケット検出手段２１は、感染表示パケットＰｂのビットにもとづいて、それが感染パケット

ＰａとＰａと検出する。ファイル実行制御手段２２は、感染パケットＰａに対応するファイルを実行不可にする。

【００１８】ウィルスパターン情報配布手段３１は、最新のウィルスパターン情報をマルチキャストでウィルスチェック装置１０ａ～１０ｎに配布する。配布されたウィルスパターンは、ウィルスパターン格納手段１１で格納される。

【００１９】ウィルスパターン情報管理手段３２は、ウィルスパターン情報の新規設定、更新等の管理を一元的に行う。次に本発明のウィルスチェックネットワーク１を、ルータで構成されているインターネット上のネットワークに適用した場合の実施の形態について以降説明する。本発明のウィルスチェック装置１０ａ～１０ｎをいくつかのルータに配置させ、ネットワーク側でウィルスチェックを行う。

【００２０】なお、ウィルスチェック装置を配置したルータを以降では、ウィルスチェックルータと呼ぶ。図２はウィルスチェックルータを配置したネットワークの概要を示す図である。ネットワーク１は、ルータＲ１～Ｒ８と、クライアント端末２０ａ～２０ｍと、ウィルス情報管理局３０と、から構成される。

【００２１】図ではルータＲ１、Ｒ２、Ｒ３、Ｒ４がウィルスチェックルータであり、その他は通常のルータ機能のみを持つ。ウィルスチェックルータＲ２にウィルス情報管理局３０が接続し、ウィルスチェックルータＲ４にクライアント端末２０ａ～２０ｍが接続する。

【００２２】ウィルスチェックルータＲ１～Ｒ４はウィルスのどの部分（先頭部、中間部、終端部）をチェックをするかを分担させており、各担当を最低１回は通過するように配置させる。

【００２３】各ウィルスチェックルータＲ１～Ｒ４は、ウィルス情報管理局３０からマルチキャストで配布されるウィルスパターンＶＰを受け取り、常に最新のウィルス情報を保持させておく。

【００２４】受信したパケットに対し、ウィルスチェックルータＲ１～Ｒ４は保持してあるウィルスパターンＶＰと比較する。もし感染している場合にはパケットにビットを立てる。

【００２５】その際同時に送信元に対しては警告パケットＰｗ１を返し、各ウィルスチェックルータＲ１～Ｒ４に対しては、警戒情報パケットＰｗ２をマルチキャストで配布する。

【００２６】警戒情報パケットＰｗ２を受け取った各ウィルスチェックルータＲ１～Ｒ４は、そのウィルスを優先的に検出、あるいは感染元との通信の遮断を行う。クライアント端末２０ａ～２０ｍでは、パケットを常に監視しており、感染を示すビットが立っている場合、あるいは警告パケットＰｗ１だった場合にはユーザにメッセージを表示し、受け取ったファイルの削除を促す。

【００２７】次にウィルスパターンＶＰについて説明する。ウィルスパターンＶＰは、マルチキャストにのせて定期的に配布される。また新種のウィルスが発見されたら、ウィルス情報管理局３０は新たに作成したウィルスパターンＶＰをマルチキャストで各ウィルスチェックルータ１０ａ～１０ｎに送り、各ウィルスチェックルータ１０ａ～１０ｎは変更があればウィルスパターンを更新する。

【００２８】図３はウィルスパターンＶＰのフォーマットを示す図である。ウィルスパターンＶＰは、ヘッダＶＰ－１にEther HedderとIP Hedder(Multicast)とを持つ。そして、ウィルスパターン配布を示すコードＶＰ－２と、ウィルスの種類を示すシリアル番号ＶＰ－３と、そのバージョン（改版番号）ＶＰ－４を持つ。

【００２９】これらのあとに、実際のウィルスのバイナリから先頭部分（第１領域のウィルスパターン）ＶＰ－６、中間部分（第２領域のウィルスパターン）ＶＰ－７、終端部分（第３領域のウィルスパターン）ＶＰ－７を固定長バイトごと抽出したものをつける。

【００３０】なお、抽出部分はウィルス情報管理局３０によって任意に決められ、定期的に変更してバージョンＶＰ－４を更新する。また、ウィルスの危険度に応じて脅威レベルＶＰ－５をウィルス情報管理局側３０で決定しておく。これにより危険度に応じた対応を可能にする。

【００３１】ウィルスチェックルータ１０ａ～１０ｎでは、受け取ったデータを元に自分の持つウィルスパターンＶＰを後述の検索テーブルに追加する。その際、各ウィルスチェックルータ１０ａ～１０ｎはどの領域を分担するか決められており、受信したパケットから自分の担当するパターンのみを受け取る。

【００３２】次にウィルスパターンＶＰの格納形式について説明する。図４はウィルスパターン格納手段１１の格納形式を示す図である。ウィルスパターン格納手段１１は、ウィルスパターンＶＰを検索テーブル１１ａと、シリアル番号保持情報１１ｂと、に分けて格納する。

【００３３】検索テーブル１１ａは、階層木構造をとる。それぞれ木の深さに応じて第１次階層、第２次階層、第３次階層…と呼ぶ。また、それぞれの枝部分とシリアル番号を対応させておく。

【００３４】シリアル番号保持情報１１ｂは、現在自分の持っているシリアル番号とバージョンと脅威レベルを保持しており、ウィルスパターンＶＰのマルチキャストパケットが来た際、これと比較して変更が必要かどうかを判断する。

【００３５】次に検索テーブル１１ａに新規にウィルスパケットＶＰを追加する場合の処理について説明する。各ウィルスチェックルータ１０ａ～１０ｎは、自分の保持しているウィルスパターンＶＰのシリアル番号と、バージョン番号と、をシリアル番号保持情報１１ｂに検索テーブル１１ａとは別に保管している。

【００３６】マルチキャストによる新規のウィルスパターンＶＰから自分の担当分を受け取ると、ウィルスパターンＶＰ情報を記録したシリアル番号保持情報１１ｂをもとにウィルスパターンＶＰの検索テーブル１１ａを更新する。

【００３７】まず、シリアル番号とバージョンをチェックして変更が必要か判断する。変更が必要と判断すると検索テーブル１１ａの第１次階層、第２次階層、…と比較していって重ならなくなる部分を探し、そこから新規に枝を伸ばす。その後、新規追加した枝を最上位に移動させ、登録を終了する。

【００３８】図５はウィルスパターン格納手段１１でのウィルスパターンＶＰを新規登録する際の処理手順を示すフローチャートである。

〔Ｓ１〕シリアル番号を自分のウィルスチェックルータ内に持っているかどうかを判断する。持っている場合はステップＳ２へ、持っていない場合はステップＳ４へ行く。

〔Ｓ２〕バージョン更新かどうかを判断する。更新ならばステップＳ３へ、更新でなければ終了する。

〔Ｓ３〕対象のシリアル番号の枝を削除する。

〔Ｓ４〕第１次階層と比較する。ステップＳ４の詳細は図６で説明する。

【００３９】図６は第ｎ次階層と比較して、新たに枝を作成する際の処理手順を示すフローチャートである。

〔Ｓ１０〕ウィルスパターンから１文字とる。

〔Ｓ１１〕既存の検索テーブル１１ａの第ｎ次階層と比較する。

〔Ｓ１２〕ヒットした場合はステップＳ１３へ、そうでなければステップＳ１４へ行く。

〔Ｓ１３〕次の第ｎ＋１次階層と比較する。

〔Ｓ１４〕枝を追加する。

〔Ｓ１５〕枝の優先順位を上にもってくる。

【００４０】以上説明したような処理手順で、新種のウィルスパターンＶＰに対して対応する枝を作成していき格納しておく。次にウィルスチェックルータ１０の構成について説明する。図７はウィルスチェックルータ１０の構成を示す図である。

【００４１】図に示す通常のパケットは、本発明のウィルスチェック手段１２に該当するウィルスチェックフィルタ１２でウィルスチェックが行われる。ここでウィルスチェックを行うべきパケットは、パケットの中身がＴＣＰかつｆｔｐ、ｈｔｔｐ、ｓｍｔｐのいずれかのパケットで、かつまだチェックが完了していないパケットである。

【００４２】ただし、それ以外のパケットは、負荷軽減のためウィルスチェックフィルタ１２をウィルスチェックせずに通過させる。また、オフセット値がある一定以上のパケット、つまりフローの後ろの方のパケットも通過させる。なお、この際ウィルスチェック済みのビットを立てる。

【００４３】一方、マルチキャストのパケットは、シリアル番号保持情報１１ｂでウィルスパターンの更新処理が行われ、検索テーブル１１ａに階層木構造形式で格納される。

【００４４】そして、経路計算部１３ａで経路計算をした後、パケット生成送信部１３ｂは、ウィルスチェックに引っかかったパケットに対して、後述のＩＰヘッダのオプションのフィールドにビットを立てた感染表示パケットＰｂを生成する。以降の同一のフローのパケットに対してもビットを立てる。

【００４５】また、パケット生成送信部１３ｂは、ＩＰパケットの送信元に向けて警告パケットＰｗ１を生成する。その後、感染表示パケットＰｂ、警告パケットＰｗ１を送信する。

【００４６】なお、警戒モードに設定して、感染元との通信を遮断する警戒モード設定手段１４については後述する。一方、クライアント端末２０では、ソフトウェアによってＩＰヘッダのウィルス感染を示すビットを監視している。ビットが立った感染表示パケットＰｂ及び警告パケットＰｗ１を受け取ったクライアント端末２０は，ユーザに対してウィルスに感染した旨のメッセージ表示を行う。

【００４７】次にＩＰヘッダの構成について説明する。図８はＩＰヘッダの構成を示す図である。バージョンは４ビットで、インターネットヘッダの形式を示す。ＩＨＬ（Internet Header Length）は４ビットで、ヘッダ長が３２ビットワード単位で示される。サービスタイプは８ビットで、スループット等のサービス品質が示される。全長は１６ビットで、オクテット単位で図った長さを示す。なお、全長にはヘッダとデータとを含む。

【００４８】識別番号は１６ビットで、送信側を識別するために割り当てられた値でデータグラムのフラグメントを組み立てる際に使用される。Flagは３ビットで、フラグメントの分割許可または継続等の制御を示す。フラグメントオフセットは１３ビットで、データグラム内でフラグメントの占める位置を示す。

【００４９】ｔｔｌは８ビットでデータグラムがインターネットのシステムに留まっていられる時間の最小値を示す。プロトコルは８ビットで、データグラムのデータ部を渡すべきトランスポートレイヤプロトコルを示す。ヘッダチェックサムは１６ビットでヘッダに対するチェックサムを示す。

【００５０】始点アドレスは３２ビットで、始点のＩＰアドレスを示す。終点アドレスは３２ビットで終点のＩＰアドレスを示す。オプションは可変長で、ユーザが任意に定義できる。本発明ではこのオプション領域を利用して感染表示パケットＰｂ、、警告パケットＰｗ１及び警戒情報パケットＰｗ２を生成する。

【００５１】次にウィルスチェック手段１２について説

明する。図９はウィルスチェックの処理手順を示すフローチャートである。

〔Ｓ２０〕すでに別のウィルスチェックルータでチェック済みかどうかを判断する。チェック済みならステップＳ３０へ、そうでない場合はステップＳ２１へ行く。

〔Ｓ２１〕オフセット値が一定以上かどうかを判断する。一定以上の場合はステップＳ３０へ、そうでなければステップＳ２２へ行く。

〔Ｓ２２〕ＴＣＰパケットでかつｈｔｔｐ、ｆｔｐ、ｓｍｔｐのいずれかのパケットかどうかを判断する。その場合はステップＳ２３へ、そうでなければステップＳ３０へ行く。

〔Ｓ２３〕ウィルスチェックを行う。なお、詳細は図１０で説明する。

〔Ｓ２４〕感染しているかどうかを判断する。感染している場合はステップＳ２８へ、そうでなければステップＳ２５へ行く。

〔Ｓ２５〕次のパケットの１バイトをとる。

〔Ｓ２６〕終了かどうかを判断する。終了の場合はステップＳ２７へ、そうでなければステップＳ２３へ戻る。

〔Ｓ２７〕チェック済みのビットを立てる。

〔Ｓ２８〕ＩＰヘッダのオプションフィールドにビットを立てる。

〔Ｓ２９〕警告パケットＰｗ１、警戒情報パケットＰｗ２を発行する。

〔Ｓ３０〕経路計算を行う。

【００５２】次に上記のステップＳ２３のウィルスチェックルーティンについて説明する。パケット内の１バイトをとり、まず検索テーブル１１ａ内の第１次階層と比較する。同じものがあった場合は、パケットから次の１バイトをとり、一致した枝の配下の第２次階層と比較する。

【００５３】もし当てはまらなくなったらパケットの次の１バイトを取り出して最初から比較をやり直す。これを繰り返し最後まで当てはまる場合は、このバイトはウィルスに感染したと判断しＩＰヘッダのオプションのフィールドのビットを立てる。

【００５４】また、もし検索の途中でパケットが終了した場合は感染していないものとみなし、代わりに別の領域を担当しているウィルスチェックルータにまかせる。図１０はウィルスチェックルーティンの処理手順を示すフローチャートである。

〔Ｓ４０〕パケットから１バイトを取り出す。

〔Ｓ４１〕パケット完了かどうかを判断する。パケット完了の場合は終了し、そうでなければステップＳ４２へ行く。

〔Ｓ４２〕ウィルスパターン第ｎ次階層と比較する。

〔Ｓ４３〕ヒットしたかどうかを判断する。ヒットした場合はステップＳ４６へ、そうでなければステップＳ４４へ行く。

〔Ｓ４４〕階層を１次に戻す。

〔Ｓ４５〕第１次階層をチェックする。

〔Ｓ４６〕階層をｎ＋１次にする。

〔Ｓ４７〕ウィルスチェック完了かどうかを判断する。完了の場合はステップＳ４９へ、そうでなければステップＳ４８へ行く。

〔Ｓ４８〕第ｎ＋１次階層をチェックする。

〔Ｓ４９〕ウィルス感染と判断する。

【００５５】次にウィルスチェック時に立てるビットについて説明する。ウィルスチェックルータでウィルスチェックを実施すると、まずＩＨＬフィールドを１増加してオプション領域を確保する。そして、確保されたオプション領域にビットを立てる。

【００５６】図１１は感染表示パケットＰｂのＩＰパケットのフォーマットを示す図である。まず、ＩＨＬフィールドを１増加する。そして、オプション領域をThe Copiedflag=0 、The option Classes=3（将来の予約用領域）、 The option Number=1（感染表示パケットＰｂ：ウィルスチェックをしたことを示すコード）、 Length=5 と設定する。

【００５７】また、Option Valueとして第１ビットは第１領域チェック未／済、第２ビットは第２領域チェック未／済、第３ビットは第３領域チェック未／済と割り当てる。すなわち、ウィルスチェックをしたかどうかの情報を記す。

【００５８】そして、第４ビットはウィルス未感染／感染を示し、未感染なら０、感染している場合は１を立てて、感染表示パケットＰｂを表す。なお、第５ビット以降はシリアル番号である。

【００５９】次に警告パケットＰｗ１について説明する。ウィルスチェックルータでウィルスを検知した際に送信元には警告パケットＰｗ１を送信し、周囲のウィルスチェックルータには警戒情報パケットＰｗ２をマルチキャストで送信する。これによってウィルスの早期発見、拡大防止をはかる。

【００６０】警告パケットＰｗ１は、ウィルス検知時のパケットと同様にＩＰヘッダのオプション領域のビットを立て、以下のフォーマットで送信元に配送される。図１２は警告パケットＰｗ１のフォーマットを示す図である。まず、ＩＨＬフィールドを１増加する。そして、オプション領域をThe Copied flag=0 、The option Classes=3（将来の予約用領域）、 The option Number=2（警告パケットＰｗ１を示すコード）、 Length=3 と設定する。そして、図１１で説明したチェック未／済のオプションを付加する。また、終点アドレスが感染元のアドレスとなる。

【００６１】次にクライアント側の処理について説明する。図１３はクライアント端末２０の構成を示す図である。本発明の感染パケット検出手段２１はＬＡＮドライバ２１ａに、ファイル実行制御手段２２はＴＣＰ／ＩＰ

ドライバ２２ｂに含まれる。

【００６２】ＬＡＮドライバ２１ａは、送られてくる各フローについて、各パケットのウィルスチェックビットを見る。そして、ビットが立っているかどうかを判断し、その結果をＴＣＰ／ＩＰドライバ２２ｂに通知する。

【００６３】ＴＣＰ／ＩＰドライ２２ｂは、ビットが立っている旨の通知を受けると、対応するファイルを実行不可にした後、ファイルを削除する旨のメッセージ２０－１を表示する。

【００６４】次にクライアント端末２０でのビット監視の流れについて説明する。図１４、図１５はクライアント端末２０のビット監視の処理手順を示すフローチャートである。

〔Ｓ５０〕パケットを読み込む。

〔Ｓ５１〕新規のフローかどうかを判断する。新規のフローの場合はステップＳ５２へ、そうでなければステップＳ５３へ行く。

〔Ｓ５２〕フロー情報を追加する。

〔Ｓ５３〕終了フローかどうかを判断する。終了フローの場合はステップＳ５４へ、そうでなければステップＳ５５へ行く。

〔Ｓ５４〕フロー情報から該当フローを削除する。

〔Ｓ５５〕ビットをチェックする。

〔Ｓ５６〕ヒットしたかどうかを判断する。ヒットした場合はステップＳ５８へ、そうでなければステップＳ５７へ行く。

〔Ｓ５７〕ＴＣＰ／ＩＰドライバ２２ｂに処理を渡す。

〔Ｓ５８〕警告パケットＰｗ１かどうかを判断する。警告パケットの場合はステップＳ５９へ、そうでなければステップＳ６０へ行く。

〔Ｓ５９〕警告の旨のメッセージを表示する。

〔Ｓ６０〕ファイルの実行権をなくす。

〔Ｓ６１〕警告メッセージ２０－１の表示を行う。

【００６５】次に警戒情報パケットＰｗ２について説明する。ウィルスチェックルータでウィルス検知された際、各ウィルスチェックルータにはマルチキャストで警戒情報パケットＰｗ２を出す。警戒情報パケットＰｗ２はウィルスパケットのシリアル番号と送信元ＩＰアドレスを情報として持ち、マルチキャストで配布される。

【００６６】警戒情報パケットＰｗ２を受け取った各ウィルスチェックルータは受け取ったシリアル番号のウィルスパターンＶＰの検索の優先順位を上げる。図１６は警戒情報パケットＰｗ２のフォーマットを示す図である。警戒情報パケットＰｗ２は、ヘッダＰｗ２－１にEther HeddとIP Hedder(Multicast)とを持つ。

【００６７】そして、警戒情報を示すコードＰｗ２－２と、ウィルスの種類を示すシリアル番号Ｐｗ２－３と、そのバージョン（改版番号）Ｐｗ２－４を持つ。さらに、ウィルスの危険度に応じた脅威レベルＰｗ２－５と、ウィルス感染元のＩＰアドレスＰｗ２－６をつける。

【００６８】次に警戒情報パケットＰｗ２を受け取った際の検索順番の処理手順について説明する。図１７は警戒情報パケットＰｗ２を受け取った際の検索順番の処理手順を示す図である。

〔Ｓ７０〕警戒情報パケットＰｗ２からシリアル番号を取得する。

〔Ｓ７１〕第１次階層、第２次階層、…第ｎ次階層、の検索順位を最上位に上げる。

【００６９】次に感染元との通信遮断を行うための警戒モード設定手段１４について説明する。脅威レベルがある一定以上の場合、拡大を防止するためウィルスチェックルータ側でホストとの通信を一定時間遮断させる。

【００７０】警戒情報パケットＰｗ２の中の脅威レベルを見て、ある一定以上の場合はＩＰアドレスをテーブルに保存し、警戒モードに移行する。警戒モードでは通常の処理の前にくるパケットをチェックし、テーブルにあるアドレスから来たパケットと、テーブルにあるアドレスに向かうパケットと、を一定時間だけすべて廃棄する。

【００７１】廃棄させる時間は、再送要求がタイムアウトする程度の時間とし、テーブルに保存された時にカウンタが一緒に設定される。もしこの時間内にパケットが来なかったらテーブルから削除し、警戒モードを解除する。逆にパケットが来たら時間（カウンタのカウント値）を延長させる。

【００７２】図１８は警戒モード設定手段１４が行う警戒モードの処理手順を示すフローチャートである。

〔Ｓ８０〕脅威レベルは一定以上かどうかを判断する。一定以上の場合は、ステップＳ８１へ、そうでなければステップＳ８９へ行く。

〔Ｓ８１〕警戒ＩＰアドレスを保持する警戒ＩＰアドレステーブルにＩＰアドレスと、警戒モードにしておく時間をカウントするカウンタ値と、を設定する。

〔Ｓ８２〕パケットを読み込む。

〔Ｓ８３〕始点／終点のアドレスがテーブルと一致するかどうかを判断する。一致する場合はステップＳ８４へ、そうでなければステップＳ８６へ行く。

〔Ｓ８４〕パケットを廃棄する。

〔Ｓ８５〕カウンタ値を延長する。すなわち、警戒モードにする時間をさらに長くする。

〔Ｓ８６〕カウンタ値を減少する。すなわち、警戒モードにする時間を短くする。

〔Ｓ８７〕カウンタを終了するかどうかを判断する。終了の場合はステップＳ８８へ、終了しない場合はステップＳ８２へ戻る。

〔Ｓ８８〕警戒ＩＰアドレステーブルからＩＰアドレスと、カウンタ値を削除する。

〔Ｓ８９〕通常モードにする。

【００７３】次にウィルスチェックルータの協調による負荷分散及びチェック精度向上について説明する。ウィルスのバイナリデータは小さく、パケットをまたがってバイナリが分割してしまう場合がある。したがって、各ウィルスチェックルータ毎に担当するウィルスパターンＶＰを異なるように分担させ保持させる。

【００７４】これにより、もしある領域で仮りにパケットの途中でウィルスのバイナリが切れてしまった場合でも、別なパケットでは別の領域のチェックにかかるようになる。

【００７５】ウィルスチェックルータに対するウィルスパターンの各分担は、手動でも自動でも設定可能とする。ただし、手動で設定する場合は、パケットは受信先に到着するまでにはすべての領域がチェックされるような構成、つまりそれぞれ分担しているウィルスチェックルータを最低１回ずつは通るような構成にする必要がある。

【００７６】次に自動で設定する場合について説明する。図１９は担当分担領域要求パケットのフォーマットを示す図である。図に示すフォーマットを用いて自動設定する。

【００７７】まず、新規のウィルスチェックルータは担当分担領域要求パケット１００を自分が配布可能な全てのウィルスチェックルータに配布する。この場合ｔｔｌ領域は小さく設定して，余計な負荷は極力かけないようにしておく必要がある。

【００７８】また、自分が持つルーティング情報から自分の接続している全ウィルスチェックルータそれぞれに対して、終点アドレスを挿入したパケットを発行する。オプション領域は、The Copied flag=0 、The option Classes=3（将来の予約用領域）、 The option Number=3（担当分担領域要求パケット１００を示すコード）、 Lngth=3 、「空き」と設定する。

【００７９】この担当分担領域要求パケット１００を受け取った各ウィルスチェックルータは、送信元に対して自分の担当領域を以下のような担当領域要求応答パケット１０１にのせて返送する。図２０は担当分担領域要求応答パケット１０１のフォーマットを示す図である。

【００８０】ｔｔｌがまだ残っていれば、自分が受け取ったウィルスチェックルータ以外の配送できる範囲の全てのウィルスチェックルータに対して同報する。担当分担領域要求応答パケット１０１のオプション領域は、The Copied flag=0 、The option Classes=3（将来の予約用領域）、 The option Number=4（担当分担領域要求応答パケット１０１を示すコード）、 Lngth=3 、「担当領域」と設定する。

【００８１】また、送信側のウィルスチェックルータは、返ってきた担当分担領域要求応答パケット１０１から各領域を担当しているルータの台数を集計して、最も担当しているルータの少ない領域を自分の担当領域とする。

【００８２】以上説明したように、本発明のウィルスチェックネットワーク１は、ウィルスチェックルータにウィルスチェック機能を搭載させることにより、ネットワーク側でウィルスを検知させることができ、ウィルス侵入防止をより多くのクライアントに対して、またより確実に行うことができる。

【００８３】また、常に最新のウィルスパターン情報をウィルスチェックルータ間でマルチキャストにより交換通知し、またその更新方法もマルチキャストのパケットを発行するだけであるので、新たなウィルスへの対応が簡単にかつ迅速に行うことができる。またクライアント側で更新をかける必要がない。

【００８４】さらに、検知したウィルスに対する警告を各ウィルスチェックルータが同時に行うことで早期発見、拡大防止を図る。そして、送信元に対しても警告パケットを送ることでウィルス感染を通知することができる。

【００８５】また、各ウィルスチェックルータでウィルスチェック領域を分担することで、各々ウィルスチェックルータにかかる負荷を分散することができ、フレーム間にまたがってウィルスが存在する場合においてもいずれかを担当しているウィルスチェックルータでチェックすることができ、ウィルスチェックの精度が向上する。

【００８６】さらに、ウィルスが検知されたパケットを落とすことはせずに、ＩＰヘッダにビットを立てて受信側に通知することで再送などによる余計なトラヒックの増加を防ぐことができる。そして、ウィルスの脅威レベルに応じて通信を遮断させるため、感染の拡大を防止させることができる。

【００８７】

【発明の効果】以上説明したように、本発明のウィルスチェックネットワークは、複数のウィルスチェック装置を設けて、ネットワーク側でウィルスチェックを行う構成とした。これにより、ネットワーク側でウィルスを未然に防ぐことができるので、ウィルスの感染及び拡大を防止でき、ウィルスチェック対策効率の向上を図ることが可能になる。

【図面の簡単な説明】

【図１】本発明のウィルスチェックネットワークの原理図である。

【図２】ウィルスチェックルータを配置したネットワークの概要を示す図である。

【図３】ウィルスパターンＶＰのフォーマットを示す図である。

【図４】ウィルスパターンＶＰ格納手段の格納形式を示す図である。

【図５】ウィルスパターン格納手段でのウィルスパターンＶＰを新規登録する際の処理手順を示すフローチャートである。

15

【図６】第ｎ次階層と比較して、新たに枝を作成する際の処理手順を示すフローチャートである。

【図７】ウィルスチェックルータの構成を示す図である。

【図８】ＩＰヘッダの構成を示す図である。

【図９】ウィルスチェックの処理手順を示すフローチャートである。

【図１０】ウィルスチェックルーティンの処理手順を示すフローチャートである。

【図１１】感染表示パケットのＩＰパケットのフォーマットを示す図である。

【図１２】警告パケットのフォーマットを示す図である。

【図１３】クライアント端末の構成を示す図である。

【図１４】クライアント端末のビット監視の処理手順を示すフローチャートである。

【図１５】クライアント端末のビット監視の処理手順を示すフローチャートである。

【図１６】警戒情報パケットのフォーマットを示す図である。

【図１７】警戒情報パケットを受け取った際の検索順番

16

の処理手順を示す図である。

【図１８】警戒モードの処理手順を示すフローチャートである。

【図１９】担当分担領域要求パケットのフォーマットを示す図である。

【図２０】担当分担領域要求応答パケットのフォーマットを示す図である。

【符号の説明】

１　ウィルスチェックネットワーク

１０ａ～１０ｎ　ウィルスチェック装置

１１　ウィルスパターン格納手段

１２　ウィルスチェック手段

１３　パケット送信手段

２０ａ～２０ｍ　クライアント端末

２１　感染パケット検出手段

２２　ファイル実行制御手段

３０　ウィルス情報管理局

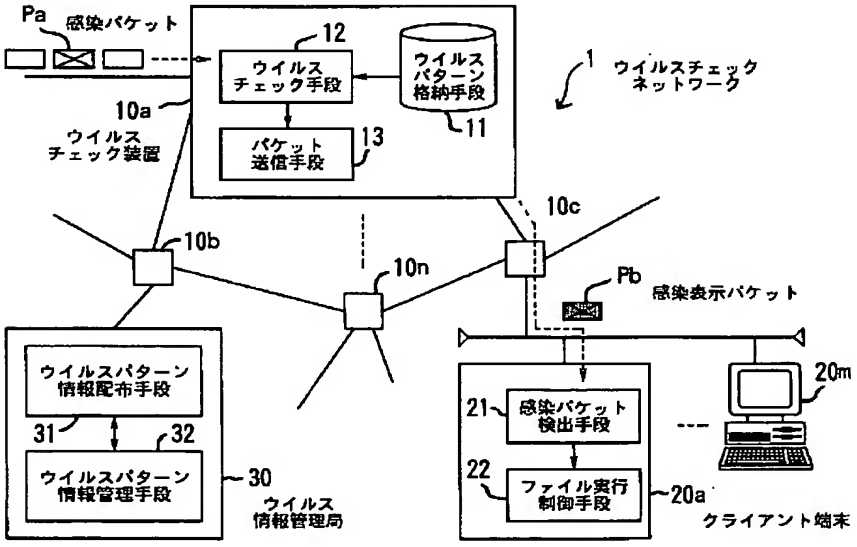
３１　ウィルスパターン情報配布手段

３２　ウィルスパターン情報管理手段

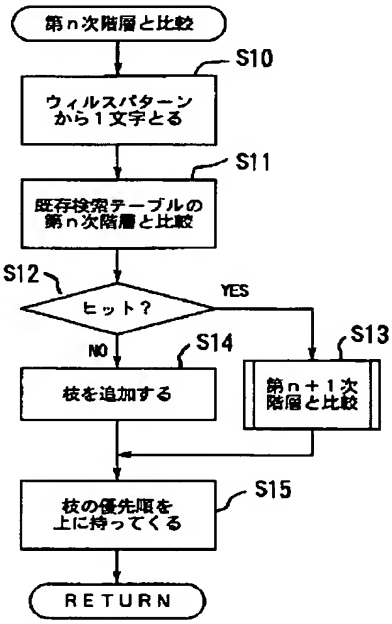
Ｐａ　感染パケット

Ｐｂ　感染表示パケット

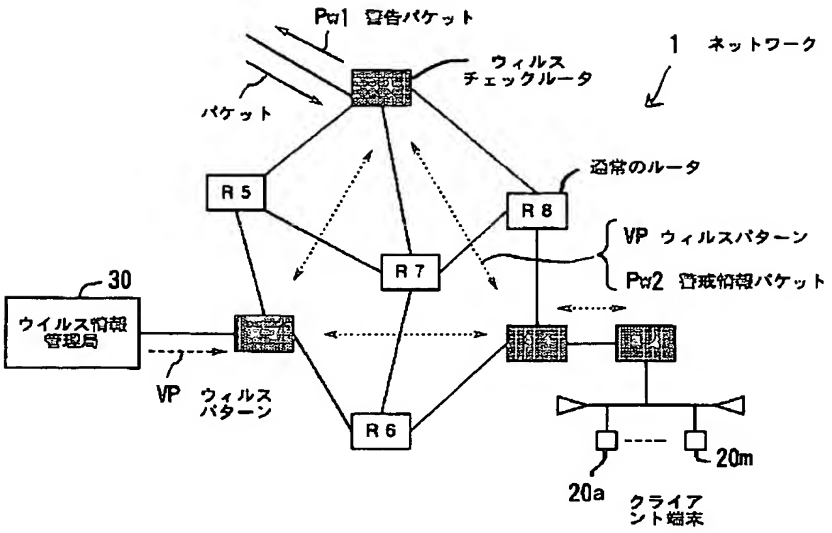
【図１】



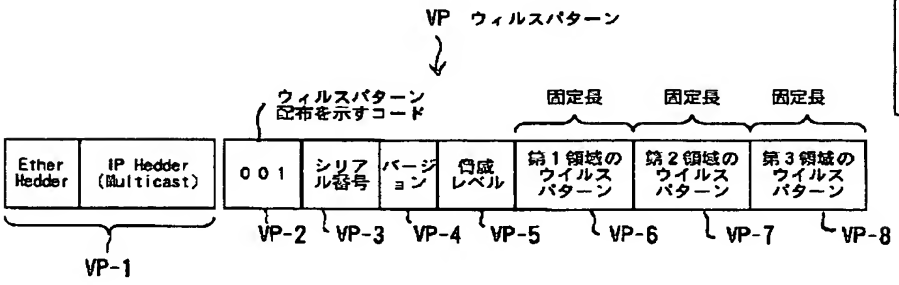
【図６】



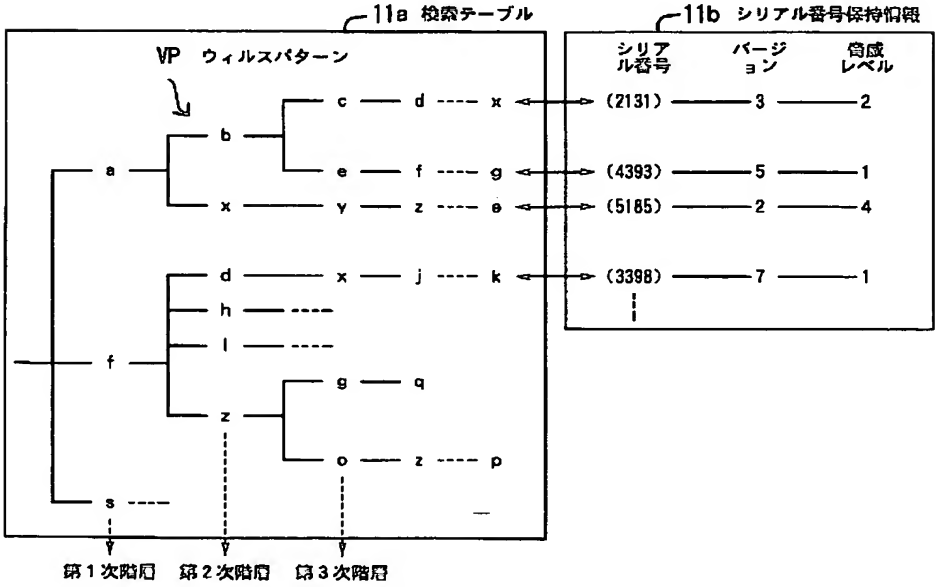
【図２】


Pw1 警告パケット
パケット
ウィルス
チェックルータ
1 ネットワーク
通常のルータ
R5
R8
R7
R6
VP ウィルスパターン
Pw2 警戒情報パケット
30
ウイルス情報
管理局
VP ウィルス
パターン
20a
20m
クライア
ント端末

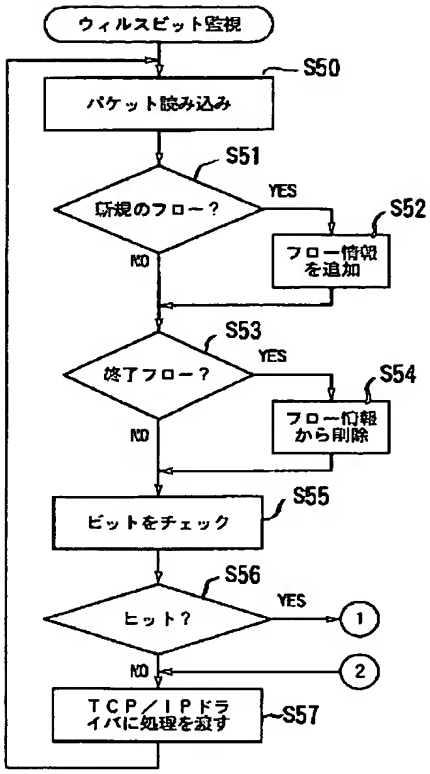
【図３】


VP ウィルスパターン
ウィルスパターン
配布を示すコード
固定長
固定長
固定長
Ether
Hedder
IP Hedder
(Multicast)
００１
シリア
ル番号
バージ
ョン
合成
レベル
第１領域の
ウイルス
パターン
第２領域の
ウイルス
パターン
第３領域の
ウイルス
パターン
VP-1
VP-2
VP-3
VP-4
VP-5
VP-6
VP-7
VP-8

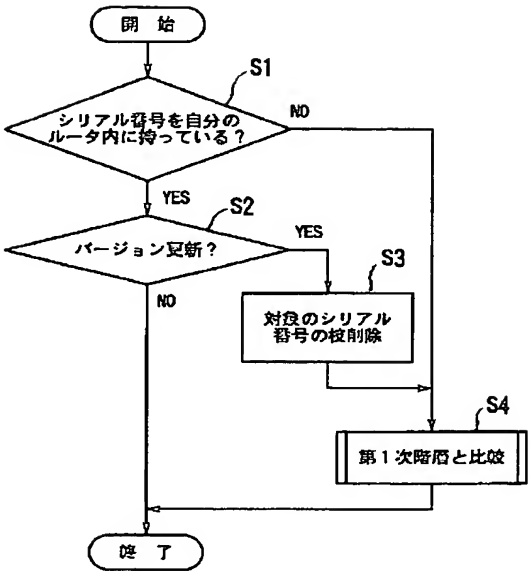
【図４】


11a 検索テーブル
11b シリアル番号保持情報
VP ウィルスパターン
シリア
ル番号
バージ
ョン
合成
レベル
(2131)
(4393)
(5185)
(3398)
第１次階層
第２次階層
第３次階層

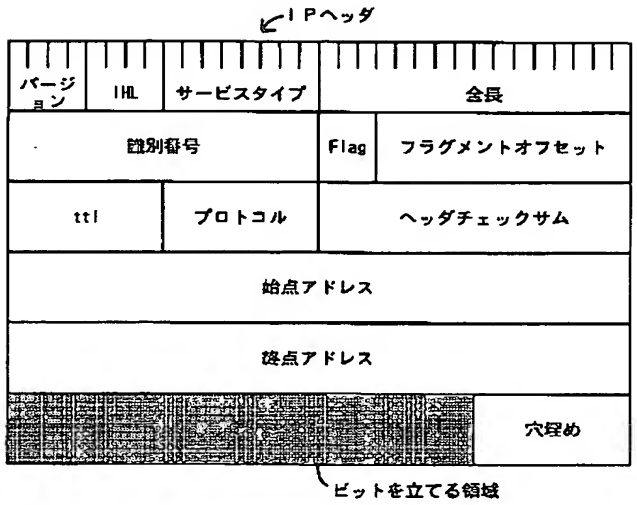
【図１４】


ウィルスビット監視
S50
パケット読み込み
S51
既規のフロー？
YES
NO
S52
フロー情報
を追加
S53
終了フロー？
YES
NO
S54
フロー情報
から削除
S55
ビットをチェック
S56
ヒット？
YES
NO
1
2
TCP／IPドラ
イバに処理を渡す
S57

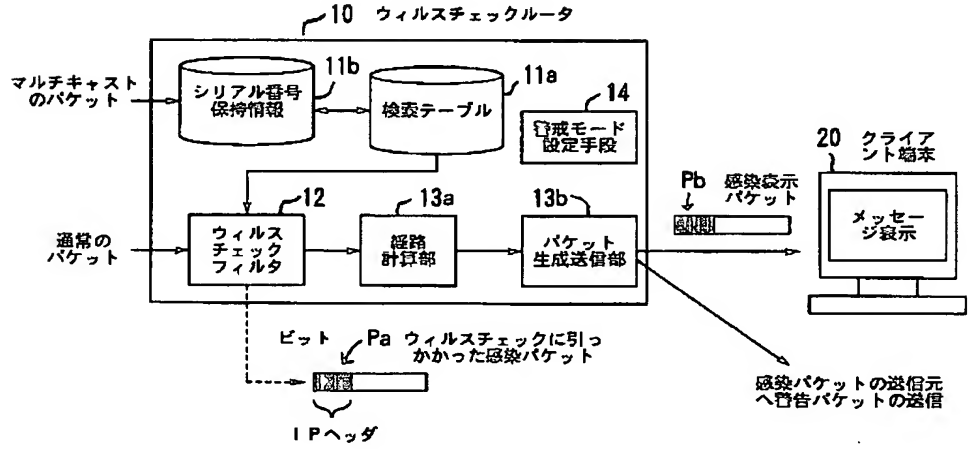
【図５】



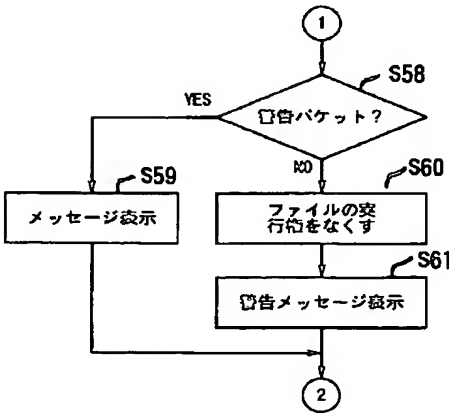
【図８】



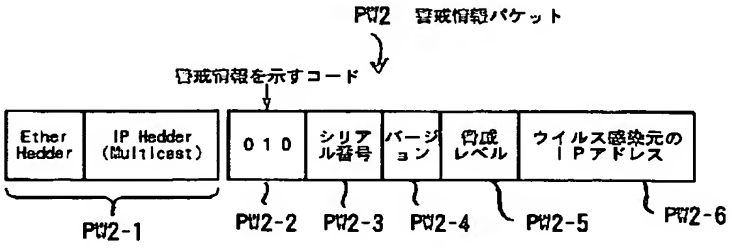
【図７】



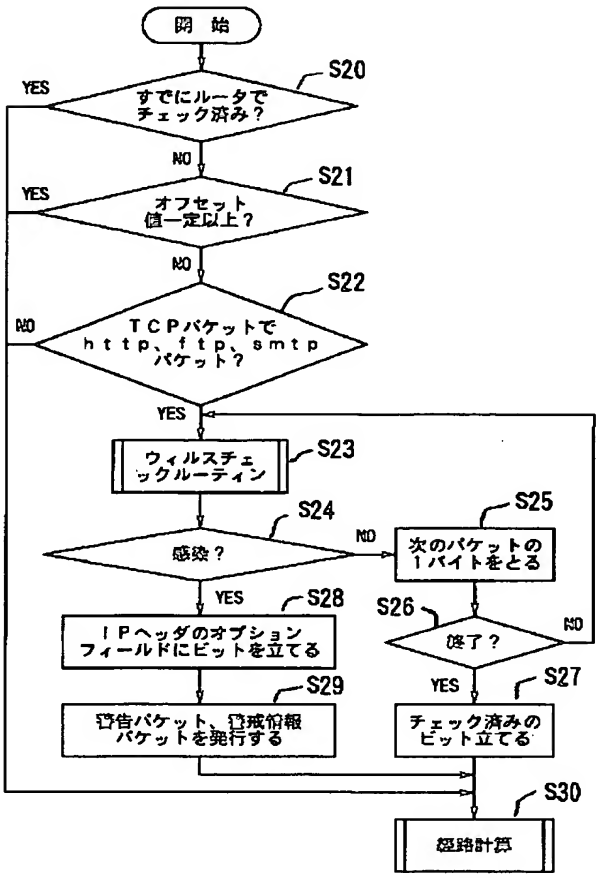
【図１５】



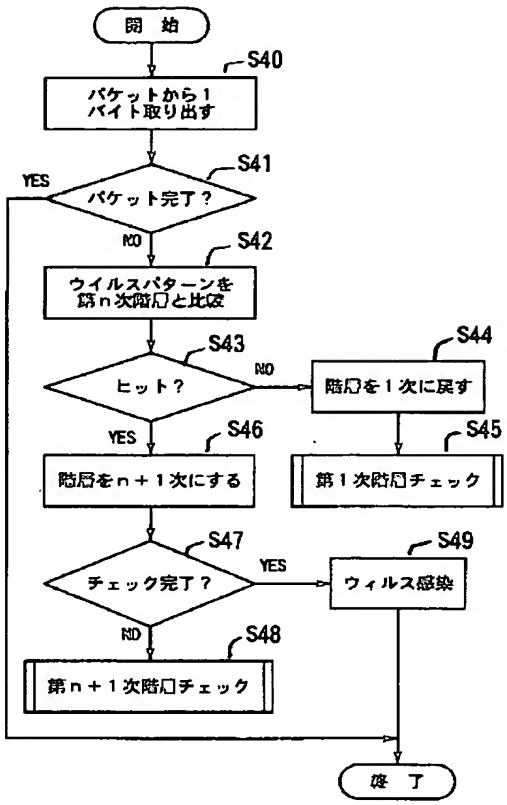
【図１６】



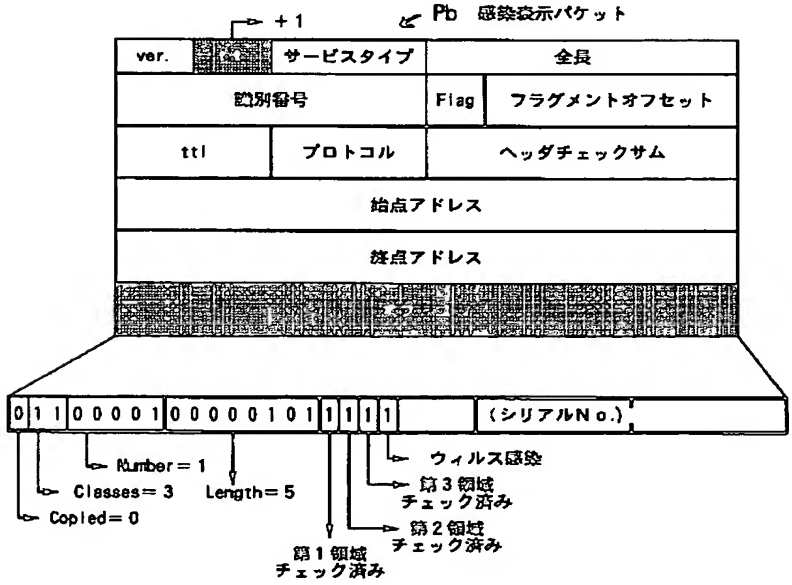
【図９】



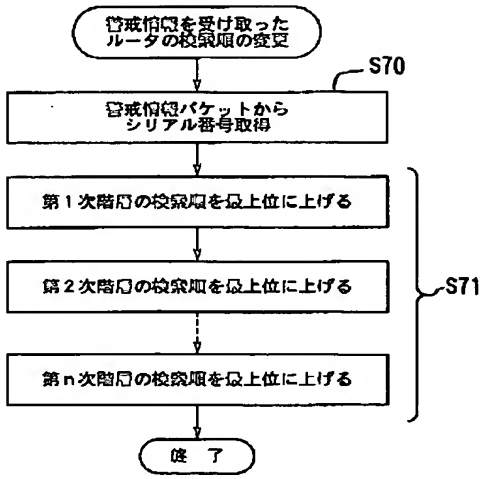
【図１０】



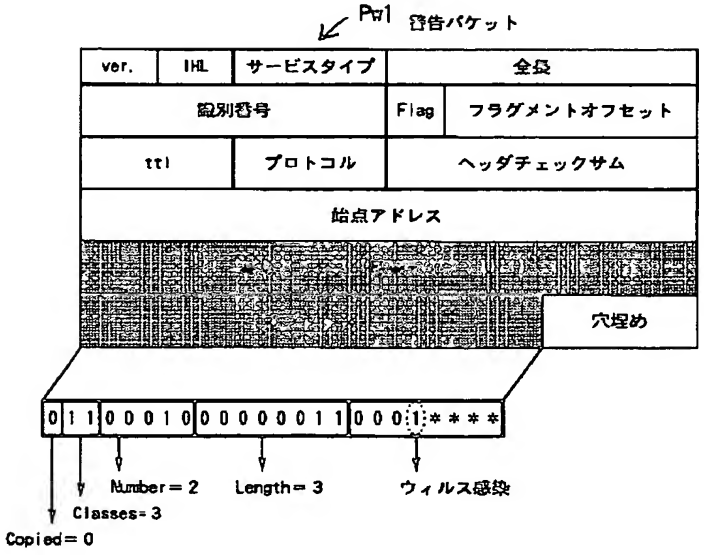
【図１１】



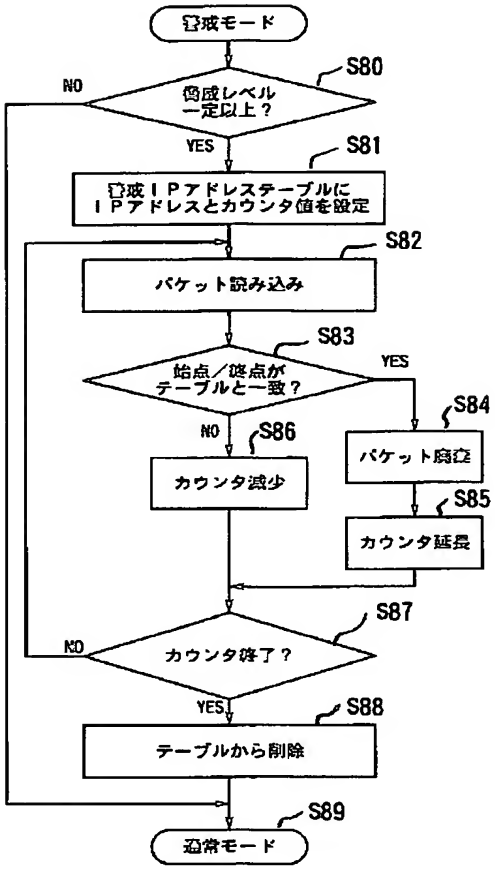
【図１７】



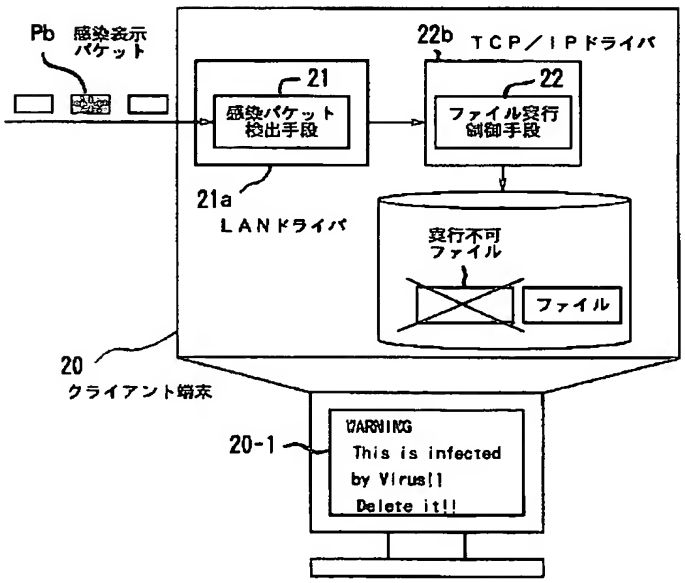
【図１２】


Pw1 警告パケット
ver.
IHL
サービスタイプ
全長
識別番号
Flag
フラグメントオフセット
ttl
プロトコル
ヘッダチェックサム
始点アドレス
穴埋め
0 1 1 0 0 0 1 0 0 0 0 0 0 0 1 1 0 0 0 1 * * * *
Number＝2
Length＝3
ウィルス感染
Classes＝3
Copied＝0

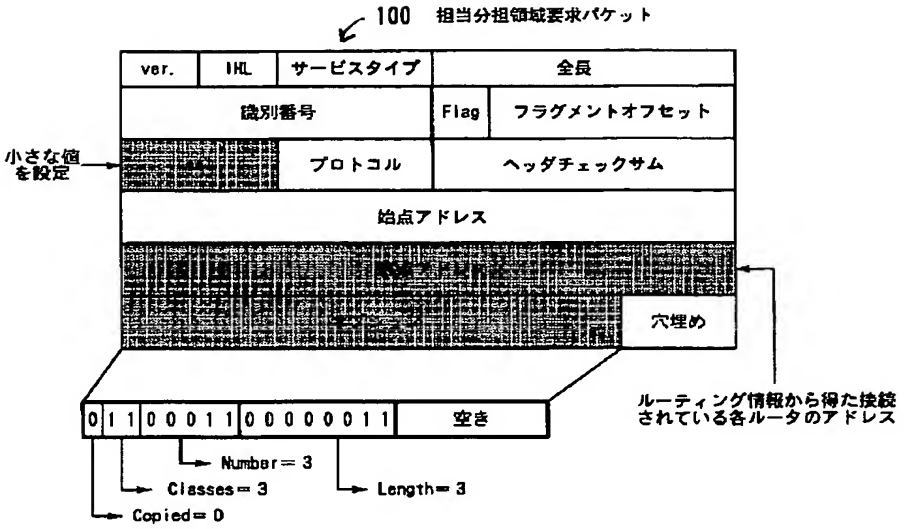
【図１８】


感染モード
S80
NO
感染レベル一定以上？
YES
S81
感染ＩＰアドレステーブルにＩＰアドレスとカウンタ値を設定
S82
パケット読み込み
S83
始点／終点がテーブルと一致？
YES
NO
S86
カウンタ減少
S84
パケット廃棄
S85
カウンタ延長
S87
NO
カウンタ終了？
YES
S88
テーブルから削除
S89
通常モード

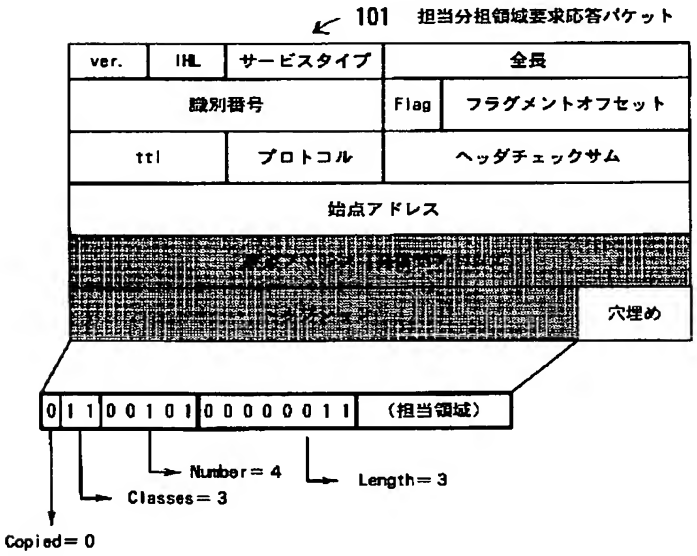
【図１３】


Pb 感染表示パケット
22b TCP／IPドライバ
21
感染パケット検出手段
22
ファイル実行制御手段
21a
LANドライバ
実行不可ファイル
ファイル
20
クライアント端末
20-1
WARNING
This is infected by Virus!!
Delete it!!

【図１９】


100 担当分担領域要求パケット
ver.
IHL
サービスタイプ
全長
識別番号
Flag
フラグメントオフセット
小さな値を設定
プロトコル
ヘッダチェックサム
始点アドレス
穴埋め
0 1 1 0 0 0 1 1 0 0 0 0 0 0 1 1
空き
ルーティング情報から得た接続されている各ルータのアドレス
Number＝3
Classes＝3
Length＝3
Copied＝0

【図２０】


101 担当分担領域要求応答パケット
ver.
IHL
サービスタイプ
全長
識別番号
Flag
フラグメントオフセット
ttl
プロトコル
ヘッダチェックサム
始点アドレス
穴埋め
0 1 1 0 0 1 0 1 0 0 0 0 0 0 1 1
（担当領域）
Number＝4
Length＝3
Classes＝3
Copied＝0

[0013]

[Embodiments] An embodiment of the present invention will be described with reference to the drawings below. Fig. 1 shows the principles of a virus check network in accordance with the present invention.

[0014] A virus check network 1 comprises virus checking devices 10a to 10n, client terminals 20a to 20m, and a virus information management station 30, and it checks for a virus so as to prevent infection by the virus.

[0015] Virus patterns are stored in a virus pattern storage means 11. A virus checking means 12 compares a received packet with the stored virus patterns, and thus performs a virus check on a network side so as to check if a received packet is a packet Pa infected with a virus.

[0016] If an infected packet Pa is detected, a packet transmitting means 13 sets a predetermined bit contained in the infected packet Pa so as to indicate infection, and transmits the packet as an infection-indicated packet Pb.

[0017] Based on the bit in the infection-indicated packet Pb, an infected packet detecting means 21 recognizes the packet as the infected packet Pa. A file execution control means 22 disables execution of a file corresponding to the infected packet Pa.

[0018] A virus pattern information distributing means 31 multicasts the latest virus pattern information to the virus checking devices 10a to 10n. The distributed virus pattern is stored in the virus pattern storage means 11.

[0019] A virus pattern information managing means 32 performs all management jobs including determination of virus pattern information and the updating thereof. Next, a description will be made of a case where the embodiment of the virus check network 1 of the present invention is adapted to a network on the Internet which comprises routers. The virus checking devices 10a to 10n employed according to the present invention are allocated to some routers in order to check for a virus on the network side.

[0020] Incidentally, the routers to which the virus checking devices are allocated shall be called virus checking routers. Fig. 2 schematically shows a network accommodating the virus checking routers. The network 1 comprises routers R1 to R8, the client terminals 20a to 20m, and the virus information management station 30.

[0021] In the drawing, the routers R1, R2, R3, and R4 are the virus checking routers, and the other routers have only the capabilities of a normal router. The virus information management station 30 is connected to the virus checking router R2, and the client terminals 20a to 20m are connected to the virus checking router R4.

[0022] The virus checking routers R1 to R4 are assigned to jobs of checking for respective parts of a virus (leading part, intermediate part, and trailing part). The virus checking routers R1 to R4 are arranged so that a packet will pass through the routers at least once.

[0023] Each of the virus checking routers R1 to R4 receives a virus pattern VP multicast from the virus information management station 30, and holds the latest virus information all the time.

[0024] Each of the virus checking routers R1 to R4 compares a received packet with the held virus pattern VP. If a received packet is infected with a virus, a bit in the packet is set.

[0025] At the same time, a warning packet Pw1 is returned to a transmitting source, and a caution information packet Pw2 is multicast to the virus checking routers R1 to R4.

[0026] Each of the virus checking routers R1 to R4 having received the caution information packet Pw2 detects the virus concerned as a top priority or discontinues communication with an infecting source. The client terminals 20a to 20m always monitor a packet. If a bit indicating infection is set or if a received packet is the warning packet Pw1, a message is displayed in order to prompt a user to delete the received file.

[0040] According to the foregoing procedure, a branch in a hierachical tree structure is created corresponding to each new kind of virus pattern VP, and then stored. Next, the configuration of the virus checking router 10 will be described. Fig. 7 shows the configuration of the virus checking router 10.

[0041] As illustrated, a normal packet is checked for a virus by a virus checking filter 12 corresponding to the virus checking means 12 employed in the present invention. Herein, a packet that should be checked for a virus is any packet which specifies TCP and ftp, http, or smtp and whose check has not been completed.

[0042] However, the other packets are passed through the virus checking filter 12 without being checked for a virus in efforts to lighten the load on the virus checking filter. A packet provided with an offset value equal to or larger than a certain value, that is, a packet to be transmitted late in a data flow is also passed. At this time, a bit indicating that a virus check has been completed is set.

[0043] On the other hand, a virus pattern specified in the serial number hold information 11b is updated with a virus pattern specified in a multicast packet. The virus pattern specified in the multicast packet is stored in the search table 11a according to a hierarchical tree structure.

[0044] After a route calculator 13a calculates a route, a packet production and transmission block 13b produces the infection-indicated packet Pb by setting the bits in an option field of an IP header of a packet that is recognized to be infected with a virus during a virus check. The bits are set in subsequent packets to be transmitted within the same data flow.

[0045] Moreover, the packet production and transmission block 13b produces a warning packet Pw1 that is duly transmitted to a transmitting source from which the IP packet has been transmitted. Thereafter, the infection-indicated packet Pb and warning packet Pw1 are transmitted.

[0046] A caution mode designating means 14 that designates a

caution mode, so as to discontinue communication with an infecting source, will be described later. On the other hand, the client terminals 20 use software to monitor a bit that is contained in an IP header in order to indicate infection with a virus. Any of the client terminals 20 having received the infection-indicated packet Pb that has the bit set and the warning packet Pw1 displays for a user a message saying that a packet has been infected with a virus.

[0047] Next, the structure of an IP header will be described. Fig. 8 shows the structure of an IP header. A version field is four bits long and specifies the format of an Internet header. An Internet header length (IHL) field is four bits long and specifies a header length in 32-bit words. A service type field is eight bits long and specifies service quality such as a throughput. An overall length field is sixteen bits long and specifies a length measured in octets. Incidentally, the overall length includes the lengths of the header and data.

[0048] An identification number field is sixteen bits long and specifies a value which is assigned to a transmitting side so that the transmitting side can be identified with the value and which is used to assemble fragments of a datagram. A flag field is three bits long and specifies that division of a fragment is enabled or continued or that control is extended in a certain manner. A fragment offset field is thirteen bits long and specifies a position in a datagram occupied by a fragment.

[0049] A time to live (ttl) field is eight bits long and specifies the minimum value of a time during which a datagram can stay in an Internet system. A protocol field is eight bits long and specifies a transport layer protocol according to which data in a datagram should be handed. A header checksum field is sixteen bits long and specifies a checksum to be adopted for a header.

[0050] A start address field is 32 bits long and specifies an IP address of a start point. An end address field is 32 bits long and specifies an IP address of an end point. An

option field has a variable length and can be defined arbitrarily by a user. According to the present invention, the option field is used to produce the infection-indicated packet Pb, warning packet Pw1, and caution information packet Pw2.

[0051] Next, the virus checking means 12 will be described. Fig. 9 is a flowchart describing a virus check procedure.

S20: It is judged whether any other virus checking router has checked a packet. If any other virus checking router has checked a packet, control is passed to step S30. Otherwise, control is passed to step S21.

S21: It is judged whether an offset value is equal to or larger than a certain value. If an offset value is equal to or larger than a certain value, control is passed to step S30. Otherwise, control is passed to step S22.

S22: It is judged whether the packet is conformable to the TCP and any of the http, ftp, and smtp. If so, control is passed to step S23. If not, control is passed to step S30.

S23: A virus check is performed. The details will be described in conjunction with Fig. 10.

S24: It is judged whether the packet is infected with a virus. If the packet is infected with a virus, control is passed to step S28. Otherwise, control is passed to step S25.

S25: One byte of the next packet is sampled.

S26: It is judged whether the byte is the last byte of the packet. If the byte is the last byte, control is passed to step S27. Otherwise, control is returned to step S23.

S27: A bit indicating that a virus check has been completed is set.

S28: The bits in the option field of an IP header are set.

S29: The warning packet Pw1 and caution information packet Pw2 are issued.

S30: A route is calculated.

[0052] Next, the virus check routine to be executed at step

S23 above will be described. One byte of a packet is sampled and compared with the first hierarchical level in the search table 11a. If the same character as the one represented by the one byte is found in the first hierarchical level, the next one byte is sampled from the packet, and compared with the second hierarchical level subordinate to the branch in which the same character as the one represented by the one byte is found.

[0053] If the same character as the one represented by one byte is not found, the next one byte is sampled from the packet and compared with the first hierarchical level again. After the comparison is repeated, if the same character as the one represented by the last one byte is found, the byte is judged to have been infected with a virus. The bits in the option field of the IP header are set.

[0054] If a packet comes to an end in the course of search, the packet is judged not to have been infected with a virus. The packet is transferred to any other virus checking router responsible for other part of a virus pattern. Fig. 10 is a flowchart describing a procedure of a virus checking routine.

S40: One byte is sampled from a packet.

S41: It is judged whether the one byte is the last one byte. If the one byte is the last one byte, the routine is terminated. Otherwise, control is passed to step S42.

S42: Another part of the packet is compared with a part of the virus pattern specified in the n-th hierarchical level.

S43: It is judged whether the search is a hit. If the search is a hit, control is passed to step S46. Otherwise, control is passed to step S44.

S44: The hierarchical level is returned to the first hierarchical level.

S45: The first hierarchical level is checked.

S46: The hierarchical level is set to the n+1-th hierarchical level.

S47: It is judged whether the virus check is completed. If the virus check is completed, control is passed to step

S49. Otherwise, control is passed to step S48.

S48: The n+1-th hierarchical level is checked.

S49: It is judged that the packet has been infected with a virus.

[0055] Next, bits to be set at the time of a virus check will be described. When a virus checking router performs a virus check, the value specified in the IHL field is incremented by one in order to preserve the option field. The bits in the preserved option field are set.

[0056] Fig. 11 shows the format of an IP packet adopted for the infection-indicated packet Pb. First, the value in the IHL field is incremented by one. The copied flag bit in the optical field is set to 0. The option class bits therein are set to represent 3 (field preserved for the future), the option number bits therein are set to represent 1 (code indicating that the infection-indicated packet Pb has undergone a virus check), and the length bits are set to represent 5.

[0057] Moreover, as an option value, the first bit is assigned to an indication that the first part of a packet has been, or has not been, checked for the first part of a virus pattern. The second bit is assigned to an indicating that the second part of the packet has been, or has not been, checked for the second part of the virus pattern. The third bit is assigned to an indication that the third part of the packet has been, or has not been, checked for the third part of the virus pattern. Namely, these bits represent the information indicating whether a virus check has been performed.

[0058] The fourth bit indicates whether the packet has been infected with a virus or not. If the packet has not been infected with a virus, the fourth bit is set to 0. If the packet has been infected with a virus, the fourth bit is set to 1. This signifies that the packet is the infection-indicated packet Pb. The fifth and subsequent bits represent a serial number.

[0059] Next, the warning packet Pw1 will be described.

After the virus checking router has detected a virus, the warning packet Pw1 is transmitted to the transmitting source concerned. The caution information packet Pw2 is multicast to the surrounding virus checking routers. This is intended to allow discovery of a virus at an early stage and to prevent expansion of infection with the virus.

[0060] The bits in the option field of the warning packet Pw1 are set similarly to those in a packet in which a virus is detected, and distributed to the transmitting source according to a format described below. Fig. 12 shows the format for the warning packet Pw1. First, the value specified in the IHL field is incremented by one. The copied flag bit in the option field is set to 0. The option class bits therein are set to represent 3 (field preserved for the future). The option number bits are set to represent 2 (code indicating the warning packet Pw1). The length bits are set to represent 3. The option value indicating, as described in conjunction with Fig. 11, whether a virus check has been completed or not is appended. Moreover, the end address is regarded as the address of an infecting source.

[0061] Next, processing to be performed on a client side will be described. Fig. 13 shows the configuration of the client terminal 20. The infected packet detecting means 21 employed in the present invention is included in a LAN driver 21a, and the file execution control means 22 therein is included in a TCP/IP driver 22b.

[0062] The LAN driver 21a checks a virus check bit in each packet transmitted during a data flow, and then judges whether the bit is set. The TCP/IP driver 22b is notified of the result of the judgment.

[0063] In response to the notification that the bit is set, the TCP/IP driver 22b disables execution of a file concerned and displays a message 20-1 saying that the file will be deleted.